WGTC 1.8p

Security Procedure

Description:

The Gramm-Leach-Bliley Act requires —financial institutions as defined by the Federal Trade Commission to protect and secure customer information such as names, social security number, addresses, account and credit card information. All of the information in the WGTC Information Security Plan comes from the Gramm-Leach-Bliley Act, the Federal Trade Commission and the lawyers who work for TCSG to protect the information of students and employees.

TABLE OF CONTENTS

Contents

I. EXECUTIVE OVERVIEW

A. What is the Gramm-Leach-Bliley Act?

The Gramm-Leach-Bliley Act (GLBA) requires —financial institutions as defined by the Federal Trade Commission (FTC), to protect and secure customer information such as names, social security numbers, addresses, account and credit card information. The GLBA also establishes a Safeguards Rule that requires the Technical College to protect and safeguard customer information.

B. What is the FTC Safeguards Rule?

The Safeguards Rule requires financial institutions to secure customer information. It requires the Technical College, as a financial institution, to develop a written information security plan that describes its program to protect customer information.

C. Why does the GLBA apply to West Georgia Technical College?

The GLBA applies to the Technical College because the Technical College is considered a —financial institution due to the financial activities in which it engages, such as processing students' financial aid.

D. What is the Scope of this Security Plan?

This Plan applies to all —customer information which is defined as any personally identifiable, nonpublic information that the Technical College handles or maintains about an individual in the process of offering a financial product or service, or such information provided to the Technical College by another financial institution. Such customer information is covered whether it is in paper, electronic or other form. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package and other miscellaneous financial services. See definition of directory data (TCSG 6.3.1p2) for a description provided by TCSG.

E. What are the Primary Goals of this Security Plan?

The primary goals of this Security Plan are to:

- Ensure the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by West Georgia Technical College;
- Develop written policies and procedures to manage and control these risks at West Georgia Technical College

- Implement and review the plan, through, among other measures, an internal audit of all security measures; and
- Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

II. COMPLIANCE MEASURES

A. Designation of Program Officer

The IT Director, is designated as the Program Officer who shall be responsible for coordinating and overseeing the procedure. The Program Officer may designate other representatives of departments within the Technical College to oversee and coordinate particular elements of the Procedure. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

B. Identifying and Assessing the Risks to Customer Information in Relevant Areas of the Technical College

Every department at West Georgia Technical College that handles or maintains customer information is responsible for identifying the type of information, the form of the information and the security risks within their department and taking appropriate measures to mitigate those risks.

West Georgia Technical College recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

West Georgia Technical College recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Program Officer will actively participate in staff development sessions and communicate with TCSG's Information Technology department regarding identification of new risks.

C. Evaluating the Effectiveness of the Current Safeguards in Place

Current safeguards taken to protect customer information include the following:

Description

- Customer information accessible only by staff with SRR on file.
- Computer access limited by system ID's and passwords
- Paper reports in file cabinets accessible only to staff in office who require access
- Offices that are locked after hours
- Data backed up nightly
- Passwords that expire periodically and employees must then reset them
- Passwords not posted in publicly viewable places nor shared with others
- Passwords must meet requirements listed in the WGTC Computer Guidelines
- Vulnerability scanning of systems containing customer information
- Antivirus protection maintained on computer systems
- Intrusion detection systems that monitor the Technical College network to allow the prompt detection of attacks and intrusions
- Separation of customer information from recycling and shredding of those records
- Referring calls or other requests for customer information to designated individuals and being alert to fraudulent attempts to obtain this information
- Keeping customer information stored in appropriate filing cabinets and clear of areas with public access

The effectiveness of the above safeguards is dependent upon

- Universal application throughout the Technical College
- Technical College employees being responsible for complying with the above safeguards
- Implementation of additional safeguards as described below

D. Implementing Supplemental Measures

Additional safeguard measures that are recommended to supplement current safeguards include the following:

Description

- Lock file cabinets containing customer information and maintain a list of persons with access to the locked cabinets
- Designate a staff member to supervise the disposal of records containing customer information in accordance with the Georgia Secretary of State's Records Retention

Rules

- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information
- When providing copies of information to others, remove non-essential and personally identifiable information that has no relevance to the transaction
- Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information in accordance with the Georgia Department of Administrative Services' rules regarding computer inventories
- Have the Program Officer conduct security reviews to identify whether additional security measures are required to protect customer information processed and stored on West Georgia Technical College Computer Systems.
- Avoid leaving computer terminals unattended when personally identifiable information is on the screen.
- Position or adapt computer terminal monitors so that personally identifiable information is visible only to the authorized user of the terminal
- Maintain inventories of all computer systems
- Reduce paper forms and documents through increased web access to this information or through internal digital imaging or document managing
- Fax machines should be in a secure or supervised area, off limits to unauthorized persons. The use of fax machines should be restricted to authorized personnel only
- Ensure the security of password protected voice mail systems.
- Ensure precautionary measures are taken when discussing personal or confidential information over the telephone.
- Centralized files
- Off-site storage retention of critical files and documents
- Implement measures to ensure unauthorized persons cannot access college computer systems when left unattended

E. Social Security Numbers

While the West Georgia Technical College Information Security Plan discourages the usage of social security numbers as student identifiers, work has been completed on the Banner Web system to change from social security numbers as student identifiers to randomly assigned student identification numbers. Therefore, by necessity, student social security numbers still remain in the West Georgia Technical College student information system. Social security numbers are considered protected information under both the Gramm-Leach-Bliley Act and the Family Educational Rights and Privacy Act (FERPA). The Program Officer will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are used, and in what instances students are being asked to provide a social security number. This assessment will cover West Georgia Technical College employees as well as possible subcontractors, for example, the bookstore and food services. The Program Officer will maintain a written record of this assessment to assist in the continuing evaluation and adjustment of this plan. (See Section VII below.)

III. EMPLOYEE EDUCATION AND TRAINING

A. Training – GTA Provided

In conjunction with Georgia Technical Authority, WGTC is actively taking part in a statewide training initiative to provide end user information, guidelines, and to relay standards to employees. Employees are required to participate in this training, and certificates of completion are maintained by HR.

B. Departmental Procedures

In conjunction with and with the assistance of TCSG, the Departments that process or maintain customer information are responsible for conducting training for employees who handle such information in the course of their job duties. This training should include physical handling and disposition of non-electronic documents containing customer information as well as proper procedures to follow in processing and storing electronic information and documents.

During employee orientation, each new employee will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Each department responsible for maintaining covered data and information should coordinate with the TCSG Information Security Office and the Office of Legal Services on an annual basis for the coordination and review of additional privacy training appropriate to the department. These training efforts should help minimize risk, and safeguard covered data and information security.

These training measures will be applicable, to the extent necessary, to all work study students.

IV. OVERSEEING SERVICE PROVIDERS

The Technical College will take reasonable steps to select and retain service providers who maintain appropriate safeguards for customer information to which the provider has access. The Office of Legal Services will take steps to ensure that all relevant contracts include a privacy clause for protected data, to be compliant with regulations.

V. PHYSICAL SECURITY

West Georgia Technical College has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information are available only to West Georgia Technical College employees with an appropriate business need for such information.

Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information are shredded at time of disposal.

VI. INFORMATION SYSTEMS

The FTC defines information systems as including network and software design, and information processing, storage, transmission, retrieval and disposal. Guidelines on how to maintain security throughout the life cycle of customer information—from data entry to data disposal are as follows:

- In order to protect the security and integrity of the Technical College network and its data, the Program Officer will develop and maintain a registry of all computers attached to the West Georgia Technical College network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the person has special access to any confidential data covered by relevant external laws or regulations.
- The Program Officer assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date, and will keep records of patching activity. The Program Officer will review its procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments are updated weekly by TCSG.
- The Program Officer bears primary responsibility for the identification of internal and external risk assessment, but all members of the West Georgia Technical College community are involved in risk assessment. The Program Officer, working in conjunction with the relevant West Georgia Technical College offices, will conduct periodic risk assessments, including but not limited to the categories listed by the Gramm-Leach-Bliley Act.
- The Program Officer will work with the relevant offices (Human Resources, the Registrar and Financial Aid, among others) to develop and maintain a registry of those members of the West Georgia Technical College community who have access to covered data and information. The Program Officer, in cooperation with Human Resources and other relevant offices will work to keep this registry up to date.
- The Program Officer will assure the physical security of all servers and terminals which contain or have access to covered data and information. The Program Officer will work with other relevant areas of West Georgia Technical College to develop guidelines for physical security of any covered servers in locations outside the central server area.
- The Program Officer will, to the extent feasible, develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks

VII. MANAGING SYSTEMS FAILURES

In the event of a breach or incident involving student PII, WGTC will adhere to TCSG guidelines and practices for notifying students and parties involved.

VIII. CONTINUING EVALUATION AND ADJUSTMENT

This Information Security Procedure will be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Program Officer who will assign specific responsibility for Information Technology implementation and administration as appropriate. The Program Officer, in consultation with TCSG's Information Security and the Office of Legal Services, will review the standards set forth in this procedure and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

IX. CONCLUSION AND ENFORCEMENT

Many privacy abuses are the result of carelessness and errors by those who handle confidential, nonpublic information. Some are caused by inadequate security. Responsible information-handling practices begin with the implementation of the safeguard measures within this procedure. Failure to implement and apply the required measures, or disregard of the implemented measures, may result in disciplinary action.

Policy Source: West Georgia Technical College	Policy Manager: Director, Information Technology	Effective: 9/2021
Division: Information Technology	Reviewed: Revised:	